

Singapore Management University
Institutional Knowledge at Singapore Management University

Centre for AI & Data Governance

SMU Institutes, Centres, Labs & Initiatives

8-2019

Data regulation with Chinese characteristics

Henry S. GAO

Singapore Management University, henrygao@smu.edu.sg

Follow this and additional works at: <https://ink.library.smu.edu.sg/caidg>



Part of the [Comparative and Foreign Law Commons](#), and the [Science and Technology Law Commons](#)

Citation

GAO, Henry S.. Data regulation with Chinese characteristics. (2019). 1-29. Centre for AI & Data Governance.

Available at: <https://ink.library.smu.edu.sg/caidg/2>

This Working Paper is brought to you for free and open access by the SMU Institutes, Centres, Labs & Initiatives at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Centre for AI & Data Governance by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Data Regulation with Chinese Characteristics

Henry Gao*

“Across the Great Wall we can reach every corner in the world”.

- *The first email sent from China on Sept 20, 1987.*

Abstract:

Data regulation has become a key issue in today’s world. For various reasons, however, it has been challenging to understand data regulations in China, home to the largest e-commerce market in the world. This paper traces the evolution of data and Internet regulation in China, from the early days of the Chinese Internet, to the regulatory turf wars among different agencies, and all the way to the elevation of data and Internet regulation to the level of national security and the rise of a super-agency in charge of the issue in recent years. The paper argues that, the Chinese Internet regulation has evolved from the regulation of the hardware and then software, to the regulation of content and now data. Through a detailed analysis of the rationale and operation of “data regulation with Chinese characteristics”, the paper aims to not only help people understand the inherent logic and mechanisms of the Chinese data regulatory model, but also find ways to deal with such regime at the international level, especially in view of the ongoing Joint Statement Initiative negotiations on electronic commerce.

Introduction

The regulation of data has become a growing feature in trade agreements. To understand

* Associate Professor, School of Law, Singapore Management University. Email: gaohenry@gmail.com. This research is supported by the National Research Foundation, Prime Minister’s Office, Singapore under its Emerging Area Research Project Funding Initiative. The author is grateful for Mira Burri for organizing the Big Data and Global Trade Law in Lucern, and Mosi Li for organizing the International Symposium on Digital Economy and Digital Trade Rules in Shanghai, where earlier versions of the paper were first presented. All errors remain the author’s own.

data regulation in trade agreements, we need to first identify the main players and interests at stake. In my view, data regulation in trade agreements mainly deal with three interests, each corresponding to different stakeholders:

The first is the commercial interests of the e-commerce firms. Due to the unique nature of their business, most Internet companies need unhindered data flows to conduct their business. Thus, they demand free flow of information across the globe, and are against data localization requirements.

Second is the person or the consumer, which supplies the raw data to use the services provided by the Internet companies. As both the raw data and processed data are controlled by the companies, consumers want to make sure that their privacy and personal data are properly protected, and this is where the third stakeholder - the state - comes into play.

The state monitors and regulates the data use by the first two groups, which involves the collection, processing, access and transfer of data. In designing the regulatory framework, the state often tries to strike a balance between the different or even conflicting interests of the different players, by trying to ensure the protection of the privacy of personal data, while not unduly hindering the development of the sector. Also, faced with various threats such as cyber-warfare and terrorism, the state also needs to ensure that public safety and national security are not compromised by rogue players roaming at large in cyberspace.

While all regulators would agree to the need to strike a balance between the clashing interests of different stakeholders, their approaches often differ in practice. Some jurisdictions prioritize the need to safeguard the privacy of users. A good example in this regard is the General Data Protection Regulation (“GDPR”) of the EU, which recognizes “[t]he protection of natural persons in relation to the processing of personal data” as “a fundamental right”.¹ On the other

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018, Recital 1.

hand, some jurisdictions put the commercial interests of firms first. In the US, this is reflected in the 1996 Telecommunication Act, which notes that it is “the policy of the United States ... to preserve ... free market ... unfettered by Federal or State regulation”.² In contrast, national security concerns are often cited to justify restrictions on cross-border data flow, albeit in varying degrees in different countries. A recent example is China’s 2017 Cybersecurity Law, which imposed several restrictions aiming to “safeguard cyber security, protect cyberspace sovereignty and national security”.³

It is not easy to say which one is the best approach, as the various regulatory approaches often reflect the different legal, political, economic, social and cultural backgrounds of different countries. What is more important than passing judgment about different models, however, is to understand the inherent logic and mechanisms of different regulatory regimes. In this chapter, I will focus on China, which is not only home to the largest e-commerce market in the world, but also has one of the most tightly-regulated cyberspaces. By providing a detailed analysis of the rationale and operation of “data regulation with Chinese characteristics”, the paper tries to help people to not only understand such regulatory model, but also find ways to deal with such regime at the international level.

I. Internet regulation in China

The first email from China was reportedly sent on September 20, 1987, by a group of researchers at the Institute for Computer Science of China's State Commission of Machine Industry to the University of Karlsruhe in Germany.⁴ On November 28, 1990, China's national domain

² Telecommunication Act of 1996, 47 U.S.C. §230(b)(2), available at <https://www.law.cornell.edu/uscode/text/47/230> (last checked 31 July 2019).

³ Cybersecurity Law of the People's Republic of China [Zhonghua Renmin Gongheguo Wangluo Anquan Fa], as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016, Art. 1, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

⁴ Li Weitao, In the beginning..., in *China Daily*, 17 March 2008, available at http://www.chinadaily.com.cn/bw/2008-03/17/content_6540460.htm (last checked 31 July 2019).

name - ".cn" - was registered by Professor Qian Tianbai, a pioneer in China's Internet industry.⁵ However, it was not until Apr 20, 1994 that the first connection to international network was established by China Education and Research Network, which marked the launch of the Internet in China.⁶

Since then, the Chinese Internet has grown by leaps and bounds, despite occasional hiccups such as Google's exit from China in 2009.⁷ In 2013, China's e-commerce volume exceeded 10 trillion RMB and it overtook the US as the largest e-commerce market in the world.⁸ Nowadays, Chinese e-commerce giants like Alibaba are among the biggest online retailers in the world and Chinese online shopping festivals such as the Singles Day (11.11) Sale have gained loyal followings all around the world.⁹ In the latest race on the research and applications of big data, machine learning and artificial intelligence, China is also quickly catching up with the US, a world leader that increasingly sees its competitive edge being narrowed.¹⁰

⁵ *Id.*

⁶ State Council Information Office [Guowuyuan Xinwen Bangongshi], China's White Paper on the State of the Internet [Zhongguo Hulianwang Zhuangkuang Baipishu], 8 June 2010, available at <http://www.scio.gov.cn/tt/Document/1011194/1011194.htm> (last checked 31 July 2019).

⁷ For a review of the background of the case and the trade law issues it raised, see Henry S. Gao, 'Google's China Problem: A Case Study on Trade, Technology and Human Rights Under the GATS', 6 *Asian Journal of WTO & International Health Law and Policy* 347 (2011), at pp. 347-385, available at SSRN: <https://ssrn.com/abstract=1976611350-356>; Henry S. Gao, 'Googling for the Trade-Human Rights Nexus in China: Can the WTO Help?', in Mira Burri & Thomas Cottier (eds.), in *Trade Governance in the Digital Age* (Cambridge University Press, 2012), pp. 247-275.

⁸ China's Bulk E-commerce Transaction Value Exceeds 10 Trillion [Woguo Dazong Dianzi Shangwu Jiaoyie Yi Chao 10 Wanyi Yuan], in *China Financial and Economic News* [Zhongguo Caijing Bao], 7 August 2014, available at http://www.mof.gov.cn/zhengwuxinxi/caijingshidian/zgcjb/201408/t20140807_1123621.html (last checked 31 July 2019). See also MOFCOM, China E-commerce Report of 2013 [Zhongguo Dianzi Shangwu Baogao 2013], available at <http://dzsws.mofcom.gov.cn/article/ztxx/ndbg/201409/20140900740745.shtml> (last checked 31 July 2019).

⁹ See Michael Smith, Australian Brands Woo Shoppers at China's Singles' Day Sales, in *Financial Review*, 12 Nov 2018, available at <https://www.afr.com/news/world/asia/australian-brands-woo-shoppers-at-chinas-singles-day-sales-20181112-h17sxb> (last checked 31 July 2019); Janice Lim, Singles' Day Sales in S'pore Doubled from a Year before: ShopBack's Data, in *Today*, 12 November 2018, available at <https://www.todayonline.com/singapore/singles-day-sales-spore-doubled-year-shopbacks-data> (last checked 31 July 2019).

¹⁰ Thomas H. Davenport, China Is Catching up to the US on Artificial Intelligence Research, in *The Conversation*, 27 February 2019, available at <http://theconversation.com/china-is-catching-up-to-the-us-on-artificial-intelligence-research-112119> (last checked 31 July 2019).

Notwithstanding the phenomenal growth in the e-commerce sector, the Internet remains under tight regulation in China. The following section provides a detailed examination of these regulations, especially those relating to the regulation of data.

1. Overview of the Regulatory Landscape

Just like the development of the Internet in China, the evolution of the regulatory landscape in China over the past 20 years is also a remarkable journey, where the haphazard regulatory patchwork was revamped in several iterations before culminating in one of the most sophisticated regulatory frameworks the world has ever seen. With the benefit of the hindsight, we can divide the development of the regulatory framework into the following four stages:

The initial stage was from 1987 to 1998, when the Internet was still in its embryonic stage and the government has yet to fully fathom its potential. Thus, the world wide web largely remained as the “wild wide web” and untangled by regulations. This does not mean that there was no regulation at all during this period. To the contrary, two important regulations were introduced in the short span of one year, *i.e.*, the 1996 Provisional Regulations on the Management of International Networking of Computer Information Networks¹¹ and the 1997 Measures for Security Protection Administration of the International Networking of Computer Information Networks.¹² However, the regulatory framework in this period suffer from the following weaknesses: First, these regulations were very low in the legislative hierarchy, as they are provisional regulations and administrative rules issued by the executive branch, which does not have the same force as national laws issued by the NPC and its Standing Committee. Moreover, these regulations were not made with the authorization of the legislature. Thus, at least in theory,

¹¹ State Council, Provisional Regulations on the Management of International Networking of Computer Information Networks [Jisuanji Xinxu Wangluo Guoji Lianwang Guanli Zanxing Guiding], Guowuyuan Ling #195, 1 February 1996, available at <http://english.mofcom.gov.cn/article/lawsdata/chineselaw/200211/20021100050748.shtml> (last checked 31 July 2019).

¹² Ministry of Public Security, Measures for Security Protection Administration of the International Networking of Computer Information Networks [Jisuanji Xinxu Wangluo Guoji Lianwang Anquan Baohu Guanli Banfa], Gonganbu Ling #33, 30 December 1997, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

these regulations may be challenged, especially with regards to the provisions that contradicts the rules in legislations of a higher rank. Second, the regulatory framework was built in a piecemeal manner. There was no central agency coordinating the powers of the different agencies, and no clear delineation of jurisdictions between the different agencies. This could potentially result in gaps and overlappings in the regulatory framework, making the whole system rather inefficient. Third, these regulations all focused on the Internet hardware and there was no regulation on the software, not to mention content. Paradoxically, this contributed to the exponential growth of the Chinese cyberspace at the turn of the century, where people flocked in pursuit of the freedom of speech unavailable offline.

The second stage started with the establishment of the Ministry of Information Industry (MII) on 31 March 1998, which results from the merger of the Ministry of Posts and Telecommunications and the Ministry of the Electronic Industry.¹³ With an explicit jurisdiction over information industry, the MII became the main regulator of the Internet.¹⁴ However, other agencies quickly stepped into the cyberspace and started to compete with MII on the regulation of various issues such as online news, audio-visual services, online media and web security.¹⁵ While these new agencies helped to fill the void in the regulatory space, their eagerness to capture more regulatory power also heightened the risk for potential turf wars. To address this, in 2001 the State Council re-established the National Informatization Leading Group.¹⁶ Headed by then Premier Zhu Rongji, the Leading Group tried to coordinate among the different agencies. In November

¹³ Li Zichen, Institutional Reforms in These Years: the Ministry of Industry and Information Technology Changed Its Name from the Ministry of Information Industry in 2008 [Jigou Gaige Zhexienian: Gongxinbu 2008 Nian you Xinxi Chanyebu Gengming Erlai], in *The Economic Observer*, 1 March 2018, available at <http://finance.sina.com.cn/china/2018-03-02/doc-ifyrztzf6047088.shtml> (last checked 31 July 2019).

¹⁴ Ministry of Information Industry [Xinxi Chanyebu], Introduction on the Ministry of Information Industry [Xinxi Chanyebu Jianjie], , 21 September 2005, available at http://www.gov.cn/banshi/2005-09/21/content_65410.htm (last checked 31 July 2019).

¹⁵ Zhu Weifeng, Changes, Challenges and Modernization of Internet Governance in China [Zhongguo Hulianwang Jianguan de Bianqian, Tiaozhan, yu Xiandaihua], in *Journalism and Communication* [Xinwen yu Chuanbo Yanjiu], No.7, 2014, at 81 , available at <http://www.hprc.org.cn/gsjj/whs/kjs/201503/P020180413574659301759.pdf> (last checked 31 July 2019).

¹⁶ Wang Yukai, The Origin and Implications of the Central Leading Group on Cybersecurity and Informatisation [Zhongyang Wangluo Anquan yu Xinxihua Lingdao Xiaozu de Youlai Jiqi Yingxiang], in *People.cn* [Renminwang], 3 March 2014, available at <http://theory.people.com.cn/n/2014/0303/c40531-24510897.html> (last checked 31 July 2019).

2004, the General Office of the CCP Central Committee and the General Office of the State Council issued Opinions on Further Strengthening Internet Administration, which clearly divided the jurisdiction and responsibilities of all central government ministries and agencies involved in Internet governance.¹⁷ However, as these agencies are all at the same ministerial-rank, the problem of regulatory competition remained. This did not change until 2010, when the General Office of the CCP Central Committee and the General Office of the State Council issued Opinions on Strengthening and Improving Internet Administration.¹⁸ Pursuant to the Opinions, the Cyberspace Administration of China ("CAC") was established in 2011 as a Ministerial-level agency.¹⁹ While its main jurisdiction is content regulation, the CAC also presides over the troika of Internet governance, which includes, in addition to the CAC, the Ministry of Industry and Information Technology (MIIT), which inherited the portfolio of the MII; and the Ministry of Public Security, which is responsible for Internet crimes and safety issues.²⁰

The third stage was heralded in 2013 by the Third Plenum Conference of the Eighteenth Party Congress, which adopted the Decision of the CCP Central Committee on Several Major Issues concerning Comprehensively Deepening Reform.²¹ The Decision adopted the policy of

¹⁷ The General Office of the CCP Central Committee and the General Office of the State Council issued Opinions on Further Strengthening Internet Administration [Zhonggong Zhongyang Bangongting, Guowuyuan Bangongting Xiaofale Guanyu Jinyibu Jiaqiang Hulianwang Guanli Gongzuo de Yijian], Zhongbanfa [2004] #32, as cited in Hu Ling, Chinese Internet Legislation before 1998 [Yijiu Jiuba Nian Zhiqian de Zhongguo Hulianwang Lifa], available at <http://www.ideobook.com/375/internet-legislation-1998/> (last checked 31 July 2019).

¹⁸ The General Office of the CCP Central Committee and the General Office of the State Council issued Opinions on Strengthening and Improving Internet Administration [Zhonggong Zhongyang Bangongting, Guowuyuan Bangongting Xiaofale Guanyu Jiaqiang he Gaijin Hulianwang Guanli Gongzuo de Yijian], Zhongbanfa [2010] #24, as cited in Tu Changbo, Generality of Broadcasting Law [Guangbo Dianshi Falv Zhidu Gailun], Beijing: Communication University of China Publishing House [Zhongguo Chuanmei Daxue Chubanshe], 2011, at p. 62.

¹⁹ The State Council Office Announced the Establishment of the National Internet Information Office--Wang Chen Is Appointed as the Director [Guoban Tongzhi Sheli Guojia Hulianwang Xinxi Bangongshi, Wangchen Ren Zhuren], in *Xinhua Press*, 4 May 2011, available at http://www.gov.cn/rsrm/2011-05/04/content_1857301.htm (last checked 31 July 2019).

²⁰ Wang Rong, Internet Governance in China in Two Decades [Zhongguo Hulianwang Jianguan Ershi Nian], in *Tencent Research Institute* [Tengxun Yanjiuyuan], available at https://www.tisi.org/4944_58 (last checked 31 July 2019).

²¹ Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform [Zhonggong Zhongyang Guanyu Quanmian Shenhua Gaike Ruogan Zhongda Wenti de Jueding], in *Xinhua Press*, 15 November 2013, available at http://www.gov.cn/jrzq/2013-11/15/content_2528179.htm (last checked 31 July 2019).

“positive adoption, scientific development, lawful administration and ensuring security” for the development of the Internet, and called for further strengthening of Internet governance, especially the further streamlining of its leadership system. Most notably, the Decision emphasized that the objective of Internet governance shall be ensuring “the security of national Internet and information”. This is the first time that Internet governance is elevated to the level of national security in a major Party document, and it sets the tone for a new era of Internet governance.

In his report to the Third Plenum meeting, President Xi covered eleven major issues, with one of them being Internet governance.²² He emphasized that Internet and information security is “a matter of national security and social stability, and a new composite challenge facing China”.²³ Xi also noted that the existing Internet governance system was lagging behind the repaid development of Internet technology and applications, and suffered from problems such as duplication and overlapping of agencies and their jurisdictions, mismatch between power and responsibilities, and low efficiency. According to Xi, to further strengthen Internet governance, the functions of the relevant agencies needs to be reshuffled to provide a comprehensive governance framework that covers everything from technology to content, and from ensuring everyday security to combating crimes.

Pursuant to the Third Plenum Decision, the Central Leading Group on Cyber Security and Informatisation was established in Feb 2014.²⁴ The Leading Group is the third “super agency” established after the Third Plenum meeting, with the other two in charge of the most important topics, *i.e.*, comprehensively deepening reform and national security, respectively. With President Xi as its head and Premier Li Keqiang the deputy, the Leading Group has 22 members, which

²² Xi Jinping, Explanations of the Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform [Guanyu Zhonggong Zhongyang Guanyu Quanmian Shenhua Gaike Ruogan Zhongda Wenti de Jueding de Shuoming], in *cpcnews.cn*, 9 November 2013, available at <http://cpc.people.com.cn/xuexi/n/2015/0720/c397563-27331312.html> (last checked 31 July 2019).

²³ *Id.*

²⁴ The Member List of the Central Leading Group on Cybersecurity and Informatisation—Staffed by Twelve National-Leader Level Leaders with Overlappings with Leading Group on Comprehensively Deepening Reform [Zhongyang Wangluo Anquan he Xinxihua Lingdao Xiaozu Chengyuan Mingdan 12 Zhengfu Guoji Jianzhi Shengaizu], in *guancha.cn* [Guanchazhe], 28 February 2014, available at http://www.guancha.cn/politics/2014_02_28_209672.shtml (last checked 31 July 2019).

includes three of the seven members of the Politburo Standing Committee, nine of the 25 members of the Politburo. Eleven of its members are also members of the Leading Group on Comprehensively Deepening Reform, one is secretary-general of the State Council at Vice Premier level, while the rest are all Ministers of important ministries, including the all-powerful National Development and Reform Commission. Such high-level set-up signals that cyber security and informatisation has been elevated to an unprecedented level and now is an important component of the overall national security strategy.²⁵ While the Leading Group remains an *ad hoc* body, it now has an office housed at the newly-restructured Cyberspace Administration of China (CAC).²⁶ This greatly elevated the status of the CAC among the peer ministries as it is one of a few agencies under the direct leadership of President Xi. In August 2014, the State Council even delegated its power on cyberspace content regulation to the CAC.²⁷ This made the CAC the most powerful agency on the regulation of Internet, especially contents.

The emphasis on cyber security was further confirmed by the 2015 National Security Law, which regards cyber security as a key component of national security and directs the state to make the “core technology of the Internet and information, key infrastructure and the information system and data in key areas secure and controllable” in order to “protect national cyberspace security, safety and development”.²⁸ Moreover, Art. 77 of the Law also requires all citizens and organizations to make timely reports on activities that engender national security, truthfully provide evidence relating to such activities that one knows of, and provide the necessary support and assistance to national security agencies. If enforced strictly, the provision could be used to

²⁵ *Id.*

²⁶ National Internet Information Office Restructured, State Council Delegated the Power on Internet Content Administration and Enforcement [Guojia Wangxinban Chongzu Guowuyuan Shouquan Qi Fuze Hulianwang Neirong Guanli Zhifa], in *guancha.cn* [Guanchazhe], 28 August 2014, available at http://www.guancha.cn/politics/2014_08_28_261572.shtml (last checked 31 July 2019).

²⁷ State Council, Notice on Delegation of Power on Administration of Internet Information Content to the National Internet Information Office [Guowuyuan Guanyu Shouquan Guojia Hulianwang Xinxi Bangongshi Fuze Hulianwang Xinxi Neirong Guanli Gongzuo de Tongzhi], Guofa [2014] #33, 26 August 2014, available at http://www.gov.cn/zhengce/content/2014-08/28/content_9056.htm (last checked 31 July 2019).

²⁸ National Security Law of the People's Republic of China [Zhonghua Renmin Gongheguo Guojia Anquan Fa], as adopted at the 15th session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on July 1, 2015, available at <http://www.chinalawinfo.com>, Art. 25 (last checked 31 July 2019).

compel netizens to report “harmful information” or activity in the cyberspace, and throw China back to the days of the Cultural Revolution, where everyone is under the constant surveillance of each other. In practice, however, this clause has yet been employed in such an aggressive manner by the authorities.

The drive on cyber-security finally culminated in the 2016 Cyber Security law, which emphasized in the first article that cyber security is a matter of cyber-sovereignty and national security. The heightened role of the CAC was also further cemented by Art. 8 of the Law, which is entrusted with the overall responsibility for the planning and coordination of cybersecurity work and relevant supervision and administration, while the other Ministries such as the MII and MPS are only responsible for the cyber-security administration within their own jurisdictions.

2. Main Regulations

From early on, the Chinese government recognized the disruptive potential of the internet and put it under strict regulation. For example, barely two years after China was connected to the internet, the State Council issued the very first internet regulation, *i.e.*, 1996 Provisional Regulations of the People’s Republic of China on the Management of International Networking of Computer Information Networks (“Provisional Regulations”).²⁹ According to Article 3, the Provisional Regulations apply to all international networking of computer information networks within China, which is defined as “networking of the computer information networks inside the People's Republic of China and those in foreign countries with the purpose of international exchange of information”. The key provision is Article 6, which provides that

“Computer information networks shall use the international entry and exit gateways provided by the Ministry of Posts and Telecommunications in the country's public telecommunications network when they carry out direct international networking. No units or individuals shall be allowed to establish or use other channels for international networking without authorization”.

²⁹ *Supra* note 12.

Anyone found in violation of the provision can be punished with a fine up to 15,000 RMB,³⁰ which is a hefty amount in 1996.

With merely seventeen articles, the Provisional Regulations seems rather rudimentary, especially considering the fact that it deals with such a complicated subject as the Internet. However, upon closer examination, we can say that it actually encapsulates all three aspects of Chinese Internet regulations for the decades to come:

The first is hardware regulation, which mandates that all Internet connections must go through official gateways sanctioned by the Chinese government. Such regulation enables the Chinese government to effectively control Internet connection, especially in blocking and filtering certain international websites and services.

The second is software regulation, which means that even the software for Internet access must be sanctioned by the government. This is hinted by Article 10 of the Provisional Regulations, which states that all individuals, legal persons and other organizations must connect to international networks through access networks, which in turn is required by Articles 8 and 6 to connect through the Internet, *i.e.*, those international gateways sanctioned by the MPT. This requirement is made explicit in the Implementation Rules for the Provisional Regulations (“Implementation Rules”) promulgated by the Leading Group for Information Technology Advancement under the State Council on 13 February 1998.³¹ After repeating the requirement to use official international gateways and the prohibition on using other gateways in Article 7, the Implementation Rules went on to state in Article 10 that all access networks to international networks shall go through the Internet and international network connections through “any other means” are explicitly prohibited. According to Article 3.3 of the Implementation Rules, the

³⁰ *Supra* note 11, Art. 14.

³¹ Information Computerization Leaders Group of the State Council, Implementation Rules for Provisional Regulations of the Administration of International Networking of Computer Information in the People's Republic of China [Zhonghua Renmin Gongheguo Jisuanji Xinxi Wangluo Guoji Lianwang Guanli Zanzing Guiding Shishi Banfa], Guoxin [1998] #001, 13 February 1998, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

international entry and exit gateways are “physical information channels used for international networking”. As Article 7 already explicitly prohibits the use of other physical gateways for connection, effective interpretation of the law means that the term “any other means” shall be interpreted broadly and includes other connection methods at both the hardware and software levels. In other words, the term “any other means” includes not only other physical gateways, but also ways to connect to the Internet through softwares such as Virtual Private Network (“VPN”). This stringent requirement is repeated in Article 12 of the Implementation Rules, which further affirms that all individuals, legal persons and other organizations must connect to international networks through access networks and not “any other means”.

The third is content regulation. Again the regulation on content is already found in the Provisional Regulations, which states in Article 13 that

“The organizations and individuals conducting international networking businesses shall abide by relevant State laws and administrative decrees and strictly follow safety and security rules. They shall use international networking for law-breaking or criminal activities that may endanger national security or divulge State secrets; or producing, consulting, duplicating or propagating information that may disturb social order or pornographic information.”

This strict regulation is also duly copied into Article 20 of Implementation Rules, with two small but significant twists. First, the subject of regulation expands from those conducting international networking businesses to the access units (ISPs) and users. This makes sense as the bulk of the content online are usually created by the intermediaries and end users. Second, the same Article also requires the three groups to immediately report any harmful information they discover to the relevant authorities and take effective measures to prevent the dissemination of such information. This is yet another important feature of Chinese Internet regulation that differs from other countries, especially the US, which do not impose liabilities on ISPs pursuant to the “safe harbour” rule. As we can see below, such approach has been extended to the regulation of data in recent years.

In the parts below, we will examine the main Chinese Internet regulations along the three themes of hardware regulation, software regulation, and content/data regulation.

1. Hardware Regulation,

According to Article 8 of the Implementation Rules, the nascent Internet in China is broken down into four networks: China Public Computer Network (CHINANET), China Golden Bridge Network(CHINAGBNET), China Education and Research Network(CERNET) and China Science and Technology Network (CSTNET), which are respectively administered by MPT, Ministry of Electronics Industry, State Education Commission, and Chinese Academy of Sciences. Among the four, the first two are commercial networks, while the last two are non-profit networks which provide Internet services for the universities and research institutes under their respective jurisdictions. In 2000, China Mobile, the largest mobile company in China, also received approval to build an international Internet gateway.³²

To further regulate international gateways, the MPT issued Administrative Rules on International Networking Entry and Exit Gateways for Computer Information Networks,³³ which further reiterated the prohibition on international networking through self-established international networking or other means including satellite.³⁴ The 2000 Telecommunication Regulation³⁵ also stated that all international telecommunication services shall go through the approved international gateways,³⁶ and explicitly prohibited operating international networking business through leasing dedicated international telecommunications lines, establishing relaying facilities without

³² Ministry of Information Industry, Approval of the Agreement to Form China Mobile Internet [Xinxi Chanyebu Guanyu Tongyi Zujian Zhongguo Yidong Hulianwang de Pifu], Xinbu Dian [2000] #48, 17 January 2000, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

³³ Ministry of Posts and Telecommunications, Notice on Issuing the Administrative Rules on International Networking Entry and Exit Gateways for Computer Information Networks [Guanyu Fabu Jisuanji Xinxi Wangluo Guoji Lianwang Churukou Xindao Guanli Banfa de Tongzhi], Youbu [1996] #492, 9 April 1996, available at <http://www.nmglib.com:8904/KCMS/detail/detail.aspx?filename=GWYB199614003&dbcode=CJFZ&dbname=> (last checked 31 July 2019).

³⁴ *Id.*, Art. 2.

³⁵ State Council, Telecommunication Regulation of the People's Republic of China [Zhonghua Renmin Gongheguo Dianxin Tiaoli], Guowuyuan Ling #291, 25 September 2000, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

³⁶ *Id.*, Art. 65.

permission or other means³⁷. To avoid confusion as to whether Internet services is part of telecommunication services, the Telecom Regulation also explicitly stated that both Internet connection service and Internet Information service are part of value-added telecom services.³⁸

When China acceded to the WTO in 2001, the hardware restriction was also copied into its Schedule of Specific Commitments on Services, which notes that “[a]ll international telecommunications services shall go through gateways established with the approval of China’s telecommunications authorities”.³⁹ There was considerable confusion as to whether China’s commitments include Internet services. On the one hand, its commitments on value-added telecom services seem to include all the value-added telecom sub-sectors under the Services Sectoral Classification List, *i.e.*, h. Electronic mail; i. Voice mail; j. On-line information and database retrieval; k. Electronic data interchange; l. Enhanced/Value-added facsimile services (including store and forward, store and retrieve); m. Code and protocol conversion; n. On-line information and/or data processing (including transaction processing). The only restriction seems to be that the services shall be provided through a joint-venture with 50% cap on foreign equity. On the other hand, China’s Telecom Regulations list Internet connection services and Internet information services separately from the value-added telecom services listed above.⁴⁰ One may argue that one of the value-added services listed in China’s schedule - on-line information and/or data processing (incl. transaction processing) - has the CPC number 843**, which corresponds to on-line content services in the current CPC version.⁴¹ However, a closer examination reveals that the correspondence is only superficial, as the two internet services under the current CPC version corresponds to 75231 and 75232 in CPC provisional (“CPCprov”),⁴² which is the basis of Services

³⁷ *Id.*, Art. 59.1.

³⁸ *Id.*, Appendix: Catalogue of Telecommunications Business.

³⁹ WTO Working Party on the Accession of China, Report of the Working Party on the Accession of China, Addendum: Schedule CLII – The People’s Republic of China, Part II – Schedule of Specific Commitments on Services, WT/ACC/CHN/49/Add.2, 1 October 2001, footnote 3.

⁴⁰ *Supra* note 38.

⁴¹ United Nations Department of Economic and Social Affairs, Statistics Division, Statistical Papers, Series M No. 77, Central Product Classification (CPC), Version 2.1, ST/ESA/STAT/SER.M/77/Ver.2.1, available at <https://unstats.un.org/unsd/classifications/unsdclassifications/cpcv21.pdf> (last checked 31 July 2019).

⁴² United Nations Department of Economic and Social Affairs, Statistics Division, CPC Versions Correspondence tables, available at

Sectoral Classification List. Class 7523 is defined in CPCprov as “data and message transmission services”, which in turn can be broken into Subclass: 75231 – Data network services, and Subclass: 75232 – Electronic message and information services.⁴³ However, according to the explanatory notes, Class 7523 only covers the necessary network services (mostly the underlying hardware) for data transmission, rather than the provision of info online. Thus, at most, China’s schedule would only cover Internet connection service but not Internet Information service. But even such an interpretation cannot get around the requirement to go through officially-sanctioned international gateways, which is repeated *ad nauseam* in the regulations mentioned above and China’s GATS schedule.

2. Software Regulation

As mentioned earlier, the Implementation Rules prohibits connection to international networks through “any other means”, which could include softwares designed to evade official international gateways in addition to hardwares. This is also copied into Article 59.1 of the Telecom Regulations, which prohibits the operation international networking business through any means. The 1997 Measures for Security Protection Administration of the International Networking of Computer Information Networks provides further clarification by prohibiting unauthorized access to or use of computer information network, which could cover access to international network using unauthorized software.⁴⁴

After Google pulled out of China in 2009, the Chinese government continued to tighten its control on cyberspace and blocked the websites of major social media (Facebook, Youtube, Twitter, etc.) and major international media (Bloomberg, Reuters, New York Times, etc.). To access these websites, many netizens resorted to VPNs. In view of this, the MIIT issued a notice

https://unstats.un.org/unsd/classifications/Econ/tables/CPC/CPCv11_CPCprov/CPCv11_CPCprov.txt (last checked 31 July 2019).

⁴³ For more detailed analysis, see Gao (2011), *supra* note 7, at pp. 361-362.

⁴⁴ Ministry of Public Security, Measures for Security Protection Administration of the International Networking of Computer Information Networks [Jisuanji Xinxì Wangluo Guoji Lianwang Anquan Baohu Guanli Banfa], Gonganbu Ling #33, 30 December 1997, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

in 2017 and explicitly prohibited VPNs.⁴⁵ To minimize the impact on firms, MIIT later clarified that foreign trade firms and multinational corporations could still lease dedicated lines for international networking from authorized telecom operators.⁴⁶ However, according to MIIT, such private networks can only be used for the internal office needs of the firm, and cannot be used to connect data centres or platforms abroad to conduct telecom businesses, which means that the lines cannot be leased to private consumers who are not employees of such firms. Since then, China has launched a major campaign to crack down on VPNs, and people have been jailed⁴⁷ and fined for selling and using VPN services respectively.⁴⁸

3. Content/Data Regulation.

The main content regulation is the 2000 Administrative Measures on Internet Information Services,⁴⁹ which states in Article 15 that Internet Information Service Provider shall not produce, copy, distribute or disseminate information that is contrary to the basic principles laid down in the Constitution, laws or administration regulations; is seditious to the ruling regime of the state or the system of socialism; subverts state power or sabotages the unity of the state; incites ethnic hostility or racial discrimination, or disrupts racial unity; spreads rumors or disrupts social order; propagates

⁴⁵ Ministry of Industry and Information Technology, Notice of the Ministry of Industry and Information Technology on Clearing up and Regulating the Internet Access Services Market [Gongye he Xinxihuabu Guanyu Qingli Guifan Hulianwang Wangluo Jieru Fuwu Shichang de Tongzhi], Gongxinbu Xinguanhan [2017] #32, available at <http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html> (last checked 31 July 2019).

⁴⁶ The Ministry of Industry and Information Technology Responded to Internet Users' Questions such as Using VPNs [Gongxinbu Huiying Wangmin VPN deng Shiyong Wenti], in *People.cn* [Renminwang], 24 January 2017, available at <http://finance.people.com.cn/n1/2017/0124/c1004-29047306.html> (last checked 31 July 2019).

⁴⁷ Benjamin Haas, Man in China Sentenced to Five Years' Jail for Running VPN, in *The Guardian*, 22 December 2017, available at <https://www.theguardian.com/world/2017/dec/22/man-in-china-sentenced-to-five-years-jail-for-running-vpn> (last checked 31 July 2019).

⁴⁸ Celia Chen, Chinese VPN User Fined for Accessing Overseas Websites as Part of Beijing's Ongoing 'Clean Up' of Internet, in *South China Morning Post*, 7 January 2019, available at <https://www.scmp.com/tech/policy/article/2180960/chinese-vpn-user-fined-accessing-overseas-websites-part-beijings-ongoing> (last checked 31 July 2019).

⁴⁹ State Council, Administrative Measures on Internet Information Services [Hulianwang Xinxu Fuwu Guanli Banfa], Guowuyuan Ling #292, http://www.gov.cn/gongbao/content/2000/content_60531.htm (last checked 31 July 2019).

feudal superstitions; disseminates obscenity, pornography or gambling; incites violence, murder or terror; instigates others to commit offences; publicly insults or defames others; harms the reputation or interests of the State; or has content prohibited by laws or administrative regulations.⁵⁰

Apparently copied from the Telecom Regulations⁵¹ and 1996 Interim Regulations on Electronic Publications,⁵² the list has remained largely constant for the past twenty years. The only addition was made in 2002, when several regulations added a new category of “harming the social morality or the excellent cultural traditions of the nationalities”.⁵³ This new category, however, seems to be restricted mainly to online publications and has not been incorporated into subsequent laws and regulations. For example, neither the Administrative Measures on Internet Information Services nor the Telecom Regulations added this new category in their 2011 and 2016 amendments. It is also worth noting that such stringent regulation is not restricted to the Internet sector, as other regulations in the same period share the same restrictions on contents.⁵⁴

⁵⁰ The translation is taken from Anne S.Y. Cheung, ‘The Business of Governance - China's Legislation on Content Regulation in Cyberspace’, 38 International Law and Politics 1 (2005-2006), at pp. 13-14, available at http://nyujilp.org/wp-content/uploads/2013/02/38.1_2-Cheung.pdf (last checked 31 July 2019).

⁵¹ *Supra* note 35, Art. 57.

⁵² General Administration of Press and Publication, Interim Regulations on Electronic Publications [Dianzi Chubanshu Guanli Zanzing Guiding], Xinwen Chubanshu Ling #6, 14 March 1996, available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

⁵³ See, e.g., General Administration of Press and Publication, Ministry of Information Industry, Interim Provisions on the Administration of Internet Publication [Hulianwang Chubanshu Guanli Zanzing Guiding], 27 June 2002, Art. 17; State Council, Regulations on the Administration of Business Sites of Internet Access Services [Hulianwang Shangwang Fuwu Yingye Changsuo Guanli Tiaoli], Guowuyuan Ling #363, 29 September 2002, Art. 14; See also Ministry of Culture, Interim Provisions on the Administration of Internet Culture [Hulianwang Wenhua Guanli Zanzing Guiding], Wenhua Ling #27, 4 March 2003, Art. 17; State Administration of Radio and Television, Measures for the Administration of the Publication of Audio-Visual Programs through the Internet or other Information Network [Hulianwang deng Xinxin Wangluo Chuanbo Shiting Jiemu Guanli Banfa], Guojia Guangbo Dianying Dianshi Zongju Ling #39, 6 July 2004, Art. 19. These regulations are all available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

⁵⁴ See State Council, Regulations of the People's Republic of China on the Administration of Audio-Visual Products [Zhonghua Renmin Gongheguo Yinxiang Zhipin Guanli Tiaoli], Guowuyuan Ling #165, 1 October 1994; State Council, Regulations on Administration of Films [Dianying Guanli Tiaoli], Guowuyuan Ling #200, 1 July 1996; State Council, Regulations on Broadcasting and Television Administration [Guangbo Dianshi Guanli Tiaoli], Guowuyuan Ling #228, 1 September 1997. These regulations are all available at <http://www.chinalawinfo.com> (last checked 31 July 2019).

One apparent gap in the 2000 Administrative Measures is that the rules apply to only Internet information service providers but not the users who generate such information. This gap is filled by the 1997 Measures for Security Protection Administration of the International Networking of Computer Information Networks, which expands the liability to “any organization or individual”.⁵⁵ In judicial practice, the offense of “Picking Quarrels and Provoking Trouble” has also been invoked on a case by case basis against people posting information online about various social problems. One example is the case of Zhao Lianhai, who was jailed for two-and-half years for trying to collect information about contaminated milk with a self-built website.⁵⁶ In 2013, the practice was further institutionalized when the Supreme People’s Court and Supreme People’s Procuratorate jointly issued a judicial interpretation, which clarifies that posting defamatory information online would be subject to the offence of criminal defamation under Article 246 of the Penal Code.⁵⁷ Moreover, in recognition of the special nature of online information dissemination, the Judicial Interpretation also states that the defamation would be consider to be “serious” if the information is clicked or browsed more than 5,000 times or forwarded more than 500 times.⁵⁸ In 2015, the Penal Code was also amended to add an additional clause in Article 291, which makes it an offence to fabricate information about natural disaster or crime and spread them online, or to spread such false information knowingly online. The issue was finally sealed when the new 2017 Cyber Security Law expanded the liability for prohibited online contents from organizations to individuals, which was repeated in two separate provisions, *i.e.*, Articles 12 and 48.

On the other hand, one could argue that such draconian laws on netizens are rather

⁵⁵ *Supra* note 12, Art. 5.

⁵⁶ Ben Blanchard, China Court Sentences Melamine Milk Activist to Jail, *Reuters*, 10 November 2010, available at <https://af.reuters.com/article/worldNews/idAFTRE6A914Y20101110> (last checked 31 July 2019).

⁵⁷ Supreme People’s Court and the Supreme People’s Procuratorate, Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate on Several Issues concerning the Application of Law in Handling Defamation and Other Criminal Cases through Information Networks [Zuigao Renmin Fayuan, Zuigao Renmin Jianchayuan Guanyu Banli Liyong Xinxi Wangluo Shishi Feibang Deng Xingshi Anjian Shiyong Falv Ruogan Wenti de Jieshi], *Fa Shi* [2013] #21, 5 September 2013, available at http://www.spp.gov.cn/spp/zd gz/201309/t20130910_62417.shtml (last checked 31 July 2019).

⁵⁸ *Id.*, Art. 2.

unnecessary, especially considering the fact that, unlike the US, the Internet information service providers are directly liable for the contents generated by users. Under the 2000 Administrative Measures, for example, the Internet information service providers are required, upon discovering prohibited information on their website, to stop the transmission, keep relevant records, and report to the relevant state authorities.⁵⁹ To give real teeth to the requirement, Article 23 of the Administrative Measures also stipulates that Internet information service providers found in violation could have their licenses revoked and websites shut down.⁶⁰

The liability for Internet information service providers was duly copied in the Cybersecurity Law.⁶¹ Moreover, it went one step further by requiring Internet information service providers to establish mechanism to facilitate online complaints and reports.⁶² A dedicated hotline and website - <http://www.12377.cn> - was also set up to handle reports on “illegal and unhealthy information”, with the first category being “political information”.⁶³ In 2018 and 2019, between 10 to 30 million reports were made on average every month, with the majority being directed against major social media sites such as Weibo, Tencent and search engines such as Baidu.⁶⁴

Another innovation in the Cybersecurity Law is the shift from the regulation of content to requirements on where such content, or data, shall be stored. According to Art. 37, operators of critical information infrastructure are required to store in China personal information and important data collected and generated in their operations within China. If they need to send such data abroad due to business necessity, they have to first undergo security assessment by the

⁵⁹ *Supra* note 49, Art. 16.

⁶⁰ *Id.*, Art. 23.

⁶¹ *Supra* note 3, Art. 47.

⁶² *Id.*, Art. 49.

⁶³ Cyberspace Administration of China (National Internet Information Office), the Center for Reporting Illegal and Bad Information [Zhongyang Wangxinban (Guojia Hulianwang Xinxi Bangongshi) Weifa he Buliang Xinxi Jvbao Zhongxin], available at <http://report.12377.cn:13225/typecatalogSelect.html> (last checked 31 July 2019).

⁶⁴ Cyberspace Administration of China (National Internet Information Office), the Center for Reporting Illegal and Bad Information [Zhongyang Wangxinban (Guojia Hulianwang Xinxi Bangongshi) Weifa he Buliang Xinxi Jvbao Zhongxin], Acceptance of National Network Reporting in June 2019 [2019 Nian 6 Yue Quanguo Wangluo Jvbao Shouli Qingkuang], 3 July 2019, available at http://www.12377.cn/txt/2019-07/03/content_40808785.htm (last checked 31 July 2019).

authorities. This provision raised several concerns. First is what constitute “critical information infrastructure”. Art. 31 defines this as those in “important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services and e-government affairs”, as well as those “that will result in serious damage to state security, the national economy and the people’s livelihood and public interest if it is destroyed, loses functions or encounters data leakage.” Such broad definition could potentially capture everything and is not really helpful, which is why the same Article also directed the State Council to develop the “specific scope of critical information infrastructure”. In 2016, the CAC issued the National Network Security Inspection Operation Manual⁶⁵ and the Guide on the Determination of Critical Information Infrastructure,⁶⁶ which clarified the scope of critical information infrastructure by grouping them into three categories: websites, which includes the websites of government and party organisations, enterprises and public institutions, and news media; platforms, which includes internet service platforms for instant messaging, online shopping, online payment, search engines, emails, online forum, maps, and audio video; production operations, which includes office and business systems, industrial control systems, big data centre, cloud-computing and TV broadcasting systems. They also laid down three steps in determining the critical information infrastructure, which starts with the identification of the critical operation, then continues with the determination of the information system or industrial control system supporting such critical operation, and concludes with the final determination based on the level of the critical operations’ reliance on such systems and possible damages resulting from security breaches in these systems. More specifically, they listed eleven sectors, which includes energy, finance, transportation, hydraulic, medical, environmental protection, industrial manufacturing, utilities, telecom and internet, radio and TV, and government agencies. The detailed criteria include both quantitative and qualitative criterion. For example, critical information infrastructure includes websites with daily visitor count of more than one million people and platforms with more than

⁶⁵ Central Leading Group on Cyber Security and Informatisation General Office, Network Security Coordination Bureau, National Network Security Inspection Operation Manual [Guojia Wangluo Anquan Jiancha Caozuo Zhinan], June 2016 (on file with author).

⁶⁶ Guide on the Determination of Critical Information Infrastructure (Trial) [Guanjian Xinxi Jichu Sheshi Queding Zhinan (Shixing)], in Notice on Conducting Network Security Inspections of Key Information Infrastructure [Guanyu Kaizhan Guanjian Xinxi Jichu Sheshi Wangluo Anquan Jiancha de Tongzhi], Zhongwangban Fawen [2006] #3, Annex 1, July 2016, available at <http://www.xxrd.gov.cn/notice/794.html> (last checked 31 July 2019).

ten million registered users or more than 1 million daily active users, or daily transaction value of ten million RMB. On the other hand, even those that do not meet the quantitative criterion could be deemed to be critical information infrastructure if there are risks of security breaches that would lead to leakage of lots of sensitive information about firms or enterprises, or leakage of fundamental national data on geology, population and resources, or seriously harming the image of the government or social order, or national security. The potentially wide reach of the criteria was well illustrated by the case of the BGI Group, which was fined by the Ministry of Science and Technology in Oct 2018 for exporting certain human genome info abroad via the internet without authorization.⁶⁷ Given the nature of their business, the BGI case could fall under the category of “leakage of fundamental national data on ...population” as mentioned earlier.

4. Summary

From the discussions above on the remarkable evolution of Internet regulation in China over the past 25 years, we can distil two key trends:

First, in terms of the institutional framework, we have seen the development from the period of no-man’s land in the 1990s, to the period of proliferation of regulation and regulators with overlapping and competing jurisdictions in the first decade of the new century. Since the beginning of the current decade, however, we have seen the power of Internet regulation consolidated into the CAC, which emerged as the dominating agency presiding over the troika of Internet governance, with the MIIT and MPS playing supporting roles.

Second, in terms of the substantive regulations, we have not only seen the initial gaps in the regulatory landscape being filled with more and more detailed regulation, but also seen the shift in the regulatory focus. At first, the regulations focused on the technology, or the hardware of the Internet. Gradually, however, the focus shifted to the software, and then to the content, and now even to the data. This moves the regulations closer and closer to the heart of the matter, as the Internet, at the end of the day, is nothing but strings of zeros and ones arranged in specific

⁶⁷ An Shujun, How to Conduct “Safety Check” for Exporting Data [Shuju Chujiing Ruhe “Anjian”], *zhihu*, available at <https://zhuanlan.zhihu.com/p/65413452> (last checked 31 July 2019).

sequences. With the adoption of the Cybersecurity Law in 2016, the focus has now been shifted to security, as the Internet is now regarded as the key challenge to the all-powerful control of the Party.

Thus, for China, Internet or data regulation has now been elevated into a matter of national security. To put it in the words of President Xi, “there is no national security without cybersecurity”.⁶⁸ Moreover, he even linked the survival of the Party with the Internet, by solemnly warning in 2013 that “unless we solve the challenge of the Internet, the Party cannot stay in power indefinitely”.⁶⁹ The key to understand data regulation in China, therefore, must be “security”. The heightened link with security not only explains the domestic regulatory framework in China, but also informs how China would deal with the issue at the international level.

II. Trade agreements

Ever since the Declaration on Global Electronic Commerce at the 2nd WTO Ministerial Conference in May 1998, WTO Members have been exploring ways to incorporate internet and data regulation into trade agreements.⁷⁰ While not much success was made in the WTO collectively, individual Members were able to address the issue in other fora such as free trade agreements and the plurilateral Trade in Services Agreement initiative.⁷¹ It makes good sense to address the issue in international trade agreements, as the Internet was born with an international nature and closely linked to commerce. At the same time, however, a country’s position on Internet and data regulation in trade agreements is often heavily influenced by its domestic regulatory

⁶⁸ The Central Leading Group on Cyber Security and Informatisation Held its First Meeting [Zhongyang Wangluo Anquan he Xinxihua Lingdao Xiaozu Diyi Huiyi Zhaokai], in *Xinhua Press*, 27 February 2014, available at http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm (last checked 31 July 2019).

⁶⁹ Xi Jinping, Speech at the National Propaganda and Thought Work Conference [Zai Quanguo Xuanchuan Sixiang Gongzuo Huiyi shang de Jianghua], 19 August 2013, as cited in Zhou Hanhua, Xi Jinping Huijianwang Fazhi Sixiang Yanjiu [Study on Xi Jinping Thoughts on Internet Legal Governance], *China Legal Science* [Zhongguo Faxue], 2017 Issue 3, at p. 7.

⁷⁰ For an overview of the issues, see Henry S. Gao, Regulation of Digital Trade in US Free Trade Agreements: From Trade Regulation to Digital Regulation (November 13, 2017). *Legal Issues of Economic Integration* 45, no. 1 (2018): 47–70. Available at SSRN: <https://ssrn.com/abstract=3070330> or <http://dx.doi.org/10.2139/ssrn.3070330>

⁷¹ *Id.*

approach, and China is no exception.

In a way, China's first encounter with data regulation in the WTO started in the wrong foot as it concerns a sensitive area: China's regulation of publications and audio-visual products.⁷² In that case, the US complained that China has failed to grant foreign firms the right to import and distribute publication and audio-visual products. One of the key issues in the case is whether China's commitments on "sound recording distribution services" covers "electronic distribution of sound recordings" as alleged by the US.⁷³ China disagreed with the US approach and argued instead that such electronic distribution "in fact corresponds to network music services",⁷⁴ which only emerged in 2001 and were totally different in kind from the "sound recording distribution services". According to China, the most fundamental difference between the two is that, unlike "traditional" sound recording distribution services, network music services "do not supply the users with sound recordings in physical form, but supply them with the right to use a musical content".⁷⁵ In response, the US cited the panel's statement in *US – Gambling*⁷⁶ that "the GATS does not limit the various technologically possible means of delivery under mode 1", as well as the principle of "technological neutrality" mentioned in the Work Programme on Electronic Commerce – Progress Report to the General Council⁷⁷, and argued that electronic distribution is merely a means of delivery rather than a new type of services.⁷⁸ Furthermore, the US argued that the term "distribution" encompasses not only the distribution of goods, but also distribution of services.⁷⁹ After a lengthy discussion covering the ordinary meaning, the context, the provisions of the GATS, the object and purpose and various supplementary means of interpretation, the Panel

⁷² Panel Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, WT/DS363/R and Corr.1, adopted 19 January 2010, as modified by Appellate Body Report WT/DS363/AB/R, DSR 2010:II, 261.

⁷³ *Id.*, at paras. 4.49-4.71.

⁷⁴ *Id.*, at para. 4.147.

⁷⁵ *Id.*, at para. 4.149.

⁷⁶ Panel Report, United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services, WT/DS285/R, adopted 20 April 2005, as modified by Appellate Body Report, WT/DS285/AB/R, DSR 2005:XII, 5797.

⁷⁷ Work Programme on Electronic Commerce, Progress Report to the General Council, adopted by the 230 Council for the Trade in Services on 19 July 1999, S/L/74, circulated 27 July 1999, para. 4.

⁷⁸ *Id.*, at para. 4.69.

⁷⁹ *Id.*, at para. 7.1156.

concluded that the term “sound recording distribution services” does extend to distribution of sound recording through electronic means.⁸⁰ China appealed the Panel’s findings, but they were upheld by the Appellate Body, which largely adopted the Panel’s reasoning.⁸¹

The case was also the first WTO case concerning China’s censorship regime. It is interesting to note, however, that the US did not challenge the censorship regime *per se*.⁸² Instead, the US only challenged the alleged discrimination in the operation of the regime, where imported products were subject to more burdensome content review requirements.⁸³ Ironically, the US even proposed, as the solution to the alleged discrimination, that the Chinese Government itself shall shoulder the sole responsibility for conducting content review, rather than outsourcing it to importing firms.⁸⁴

With such unpleasant experience, China took a cautious approach on the inclusion of Internet or data regulation in other fora, such as free trade agreements. While it has signed more than a dozen FTAs so far, most of them have not included provisions on such regulations. The only exceptions are the two FTAs China signed with Korea and Australia⁸⁵ in 2015, which both included stand-alone chapters on e-commerce. However, unlike the US FTAs, which often include provisions on free flow of data and ban on data localisation requirements,⁸⁶ the two FTAs only address e-commerce related issues such as moratorium on customs duties on electronic transmission; electronic authentication and electronic signature; protection of personal information in e-commerce; and paperless trading.⁸⁷ Thus, they do not really address Internet and data

⁸⁰ *Id.*, at para. 7.1168-1265.

⁸¹ Appellate Body Report, China – Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, WT/DS363/AB/R, adopted 19 January 2010, DSR 2010:I, 3, at paras. 338-413.

⁸² ABR, para. 20.

⁸³ Panel report, para. 4.72-4.85.

⁸⁴ Panel report, Para. 7.875; AB report, para. 72.

⁸⁵ See also Henry Gao, E-Commerce in ChAFTA: New Wine in Old Wineskins?, in Colin Piker, Heng Wang & Weihuan Zhou (eds.), *The China Australia Free Trade Agreement: A 21st-Century Model*, Hart, 2018, 283-303.

⁸⁶ See Gao, *supra* note 70.

⁸⁷ See Henry S. Gao, Digital or Trade? The Contrasting Approaches of China and US to Digital Trade (December 28, 2017). *Journal of International Economic Law*, Volume 21, Issue 2, 1 June 2018, Pages 297-321, DOI:

regulation issues as such.

A similar approach is taken by China in WTO negotiations. Even though the US has long been calling for rules on issues such as free cross-border data flow and ban on data localisation requirements, China has ignored these issues until very recently. For example, in its communication on e-commerce jointly tabled with Pakistan before the 11th Ministerial Conference, China focused only on “cross-border trade in goods enabled by internet, together with services directly supporting such trade in goods, such as payment and logistics services”.⁸⁸ As I mentioned in another paper, such approach is a reflection of the different nature of business of most Chinese Internet firms, as they tend to focus on trade in physical goods facilitated by the Internet, rather than digital products like Google and Netflix.⁸⁹ Thus, when 70+ WTO Members issued a joint statement on launching the negotiations on e-commerce at the 11th Ministerial Conference in Dec 2017,⁹⁰ China declined to join. When these Members decided to formally launch the e-commerce negotiations in January 2019, however, China changed its position and jumped on the negotiation.⁹¹ In April 2019, China issued a communication on the joint statement negotiation, in which it repeated the focus on cross-border trade in goods enabled by the internet.⁹² At the same time, however, it also addressed the main concerns of the US, *i.e.*, data flow, data storage, treatment of digital products, *etc*, in the following manner:

First, rather than ignoring these issues as it has done in the past, China chose to face them and acknowledge them as issues of concern for some Members. This itself is a positive sign, as it

10.1093/jiel/jgy015. Available at SSRN: <https://ssrn.com/abstract=3162557> or <http://dx.doi.org/10.2139/ssrn.3162557>.

⁸⁸ WTO General Council, Council for Trade in Goods, Council for Trade in Services, Committee on Trade and Development, Work Programme on Electronic Commerce: Aiming at the 11th Ministerial Conference, Communication from the People's Republic of China and Pakistan, Revision, JOB/GC/110/Rev.1, JOB/CTG/2/Rev.1, JOB/SERV/243/Rev.1, JOB/DEV/39/Rev.1, 16 November 2016.

⁸⁹ See Gao, *supra* note 87.

⁹⁰ WTO, Joint Statement on Electronic Commerce, Ministerial Conference, Eleventh Session, Buenos Aires, 10-13 December 2017, WT/MIN(17)/60, 13 December 2017.

⁹¹ Leika Kihara, DAVOS-Nearly half WTO members agree to talks on new e-commerce rules, *Reuters*, 25 January 2019, available at <https://www.reuters.com/article/davos-meeting-ecommerce/davos-nearly-half-wto-members-agree-to-talks-on-new-e-commerce-rules-idUSL1N1ZP08O>.

⁹² WTO, Joint Statement on Electronic Commerce: Communication from China, INF/ECOM/19, 24 April 2019.

indicates China's willingness to engage on these issues.

Second, at the same time, China also indicated that it was not ready to discuss these issues, at least not in the early stages of the negotiation. Citing the "complexity and sensitivity" of these issues, as well as "the vastly divergent views among the Members", China stated that "more exploratory discussions are needed before bringing such issues to the WTO negotiation, so as to allow Members to fully understand their implications and impacts, as well as related challenges and opportunities." Such approach is all too familiar to those who follow WTO negotiations closely, as it is basically a polite way of saying "we don't want to discuss these issues now".

Third, in particular, China singled out the issue of cross-border data flow, by stating that "[i]t's undeniable that trade-related aspects of data flow are of great importance to trade development". It is interesting to note, however, what China did and did not say in this sentence. It did not, for example, use "free flow of data", which is how the US has always referred to the issue in its submissions.⁹³ On the other hand, it qualified "data flow" with "trade-related aspects". This implies that China is not willing to address all kinds of data flows, just those related to trade. In other words, to the extent that some data flows do not have a trade nexus, they could be legitimately excluded. As I mentioned in another article, this qualification could have wide implications as it could be employed to justify restrictions on data flows in sectors that China have not made commitment, or even for those covered by existing commitments but are provided free of charge (such as Google's search engine services) as they are not "traded".⁹⁴

Fourth, in an effort to turn the table, China also prefaced the discussion on these "other issues" with the recognition that Members shall have the "legitimate right to adopt regulatory measures in order to achieve reasonable public policy objectives". This language is reminiscent of the calls for more "policy space", a term often employed in trade negotiations to justify special and differential treatment and resort to exceptions clauses. As the *China – Publications and Audiovisual* case mentioned above has illustrated, China will, most likely, invoke the public order exception contained in the General Exceptions clauses of both the GATT and GATS to justify its online censorship regime. In particular, on data flow, China emphasized that it "should be subject to the precondition of security", and should "flow orderly in compliance with Members' respective

⁹³ See JOB/GC/94, which refers to "free flow of information" in para. 2.3, and INF/ECOM/5, which refers to "free flows of information" in Section 2.

⁹⁴ Gao, *supra* note 87.

laws and regulations”. This extends China’s domestic narrative of cybersecurity to the international level, which is made complete with the earlier reference for all Members to “respect the internet sovereignty” of other Members. By elevating the issue to one of “sovereignty”, China has shown the seriousness it attaches to the issue of regulating data flow.

In summary, China has made it clear that it was yet ready to discuss these sensitive issues, at least not in the early stages of the negotiations. There is a possibility that it will consider some of the issues further down the road, but such negotiations will not be easy given China’s guarded position on these issues.

III. Conclusion

When people discuss data regulations today, they tend to focus on two main players: the US, which calls for free flow of data to serve the interests of firms; the EU, which prioritize the need for the protection of personal information and privacy of the consumers. This paper discusses the third major player - China - which emphasizes on data security and even regards it as a matter of national sovereignty. Of course, such regulatory approach was not formed overnight. Instead, the discussions above have illustrated how such “data regulation with Chinese characteristics” evolved over the past 25 years. More specifically, the analyses in this paper have shown the differing regulatory logics and approaches at two different levels.

First, at the domestic level, we have seen Internet regulation shifting from hardware to software, and now to content and data. The shift in regulatory focus closely follows the development of the Internet in China, where it started as a novelty that is confined to the ranks of tech-savvy geeks, then gradually expands to the masses with the proliferation of softwares and apps catered to popular uses, and now permeates everyone’s daily life from socialising, shopping to entertainment and education. Recognising the central role played by the Internet in the modern life, the Chinese regulators have shrewdly chosen to regulate data, which is the essence of cyberspace that powers everything, especially with the rise of big data and artificial intelligence. Moreover, data regulation has now been elevated to the level of national security, and the agency that is responsible for content regulation, the CAC, has also evolved into the super-agency that is

almost synonymous with data regulation in China. The CAC has no responsibility in promoting the growth of the sector. Instead, their only responsibility is making sure that the cyberspace is secure and nothing unexpected would pop up. It is this single-minded pursuit of security that led to such draconian policies as Internet blockage, filtering and other restrictions on free flow of data, and forced data localization requirements and forced transfer of source code. As the Internet is becoming more complicated and omnipotent, we can only expect Internet and data regulations in China becomes more sophisticated and omnipresent.

Second, at the international level, China has for a long time been rather cautious in addressing Internet and data related issues, due to its unpleasant experience in WTO disputes. Such approach is also reflected in its free trade agreements, which tends to avoid these issues. Even though its most recent free trade agreements, especially the ones with Korea and Australia, started to address these issues, they tend to focus on only e-commerce related issues and do not really address data flow issues. At the same time, in contrast to its defensive position on data-related issues, China has been quite aggressive in pushing for liberalization of “cross-border trade in goods enabled by internet”. This reflects China’s interest as the leading goods exporter and the success of its e-commerce platforms such as Alibaba. In its latest proposal on the WTO Joint Statement Initiative on e-commerce, China started to address data regulations, but they are framed as secondary issues that require “more exploratory discussions” and are subject to each Member’s “right to regulate” to achieve other policy goals, especially security.

The growth of the internet in China over the past 25 years has not only led to the phenomenal growth of its e-commerce market, but also gave China the confidence and power to export its model, and to “set the agenda and make rules for cyberspace at the international stage”, as per the high-level exhortation by President Xi at the Politburo’s 36th Collective Study Session on “Implementation of the Internet Power Strategy” in Oct 2016.⁹⁵ The success of China’s e-commerce sector will make the Chinese model attractive to many developing countries, as many

⁹⁵ Xi Jinping: Accelerate the Promotion of Indigenous Innovation on Internet Information Technology, Strive Unrelentingly Towards the Objective of Building the Internet Power [Xi Jinping: Jiakuai Tuijin Wangluo Xinxi Jishu Zizhu Chuangxin, Chaozhe Jianshe Wangluo Qiangguo Mubiao Buxie Nuli], in *Xinhua News*, 9 October 2016, available at http://news.xinhuanet.com/politics/2016-10/09/c_1119682204.htm (last checked 31 July 2019).

of them are trying to emulate the accomplishments of China. However, an argument could be made that given China's huge population base and the resulting enormous market, its e-commerce success story is more in spite of, rather than because of, the tight grip on the cyberspace by the government. Nonetheless, given China's growing economic clout, data regulation with Chinese characteristics is something that the rest of the world must grapple with for some time to come. It is in this regard that this chapter tries to make some contributions by offering a preliminary peek behind the cyber curtain, while offering some hints on things to come.